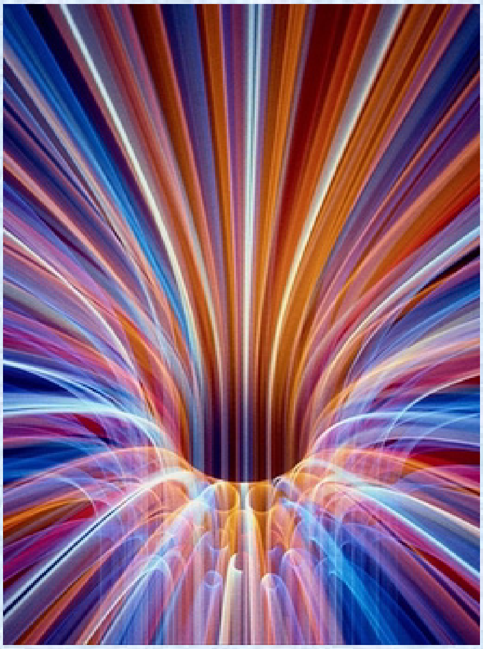
Cyber Security

A collection of countermeasures to protect information systems and the data they store, process, or distribute from unauthorized access, alteration or destruction, and denial of services



Providing a safe and secure cyber environment is recognized as one of the most important and challenging needs of government and business today. The threat spectrum, in order of increasing motivation and resources, includes system users, hackers, criminal elements, and foreign agents. For security measures to be effective, they must be considered over the entire life cycle of an information system from design to deployment.

The Networking and Security Group of the Technical Computing organization has extensive capabilities in virtually every facet of cyber security, including vulnerability and risk assessments, system design, security planning, security testing and evaluation, user security training and awareness, and ultra-secure computer networks. A number of staff members are certified as information security professionals.

Capabilities

- Secure Network Design
- Security Plans and Documentation
- Vulnerability and Risk Assessments
- Security Products Evaluations
- Security Training
- Encryption
- Public Key Infrastructure
- Security Testing
- Advanced Authentication
- Healthcare Information Security
- Policy Evaluation

Y12 National Security Complex

Cyber Security guards against system users, hackers, criminal elements, and foreign agents.

Protection includes encryption and detection devices.

User training provides awareness of individual responsibilities for protecting sensitive information.

Applications

The Networking and Security Group has provided cyber security support to a broad customer group with applications across the federal government, including DoD, DOE, NNSA, FBI, OPM, and the State Department. The integration of networking and cyber security expertise provides cost-effective support for the design, development, deployment, and evaluation of secure information systems. Network and cyber security support applications have been provided in the following areas:

- Certification practice statement documents for PKI for unclassified and classified networks
- Cyber security policy assessment
- Intrusion detection concept of operations
- FBI INFOSEC training for information security officers
- Firewalls, intrusion detection systems, and public key infrastructure products
- Computer security plans and other security documentation
- Security testing and evaluation for certification and accreditation for a three-site classified and unclassified network
- Inspection, verification and validation of cyber security
- Alarm systems for highly classified environments
- Evaluation of biometric technologies for secure access control
- Penetration testing (PT) for FBI computer systems.
- Information technology vulnerability assessments for the FBI, DOE, DoD, law enforcement agencies and electric utilities
- Security assessments of law enforcement information systems

For more information, contact:

Bob Ervin
(865) 574-0615
ervinrs@y12.doe.gov

Y-12 National Security Complex
Oak Ridge, Tennessee

Rev. 0 3/2003